Amendments to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for password-based authentication in a communication system including a group of at least two units associated with a common password, comprising the steps of:

assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;

determining, at a first unit, a check token for a second unit based on the password inputted by a user of said first unit and the authentication token of the first unit, wherein the step of determining the check token comprises the steps of:

~~retrieving~~ determining, at the first unit, a token secret using the authentication token of the first unit and the password; and,

creating, at the first unit, the check token for the second unit based on the token secret and the password; [[and]]

sending the check token to the second unit; and,

comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit, wherein said user of said first device is authenticated if said check token is the same as said authentication token of said second unit.

2. (Currently Amended) The method of claim 1, further comprising the step of:

deleting the password and all significant parameters generated in the authentication procedure except the authentication tokens after usage thereof.

3. (Currently Amended) The method of claim 1, further comprising the step of:

accepting, at the second unit, in response to a successful authentication, update information securely transferred from the first unit, at least a portion of the update information being created at the first unit.

4. (Previously Presented) The method of claim 3, wherein the update information is associated with revocation of a non-trusted group member.

5. (Previously Presented) The method of claim 3, wherein the update information relates to a password change.

6. (Currently Amended) The method of claim 3, wherein the update information is selected from the group of:

new authentication tokens,

a new group key, a group-defining list, and,

a revocation list, including combinations thereof.

7. (Previously Presented) The method of claim 3, further comprising the step of delegating update rights to a third intermediate unit, and sending at least a portion of the update information for the second unit to the intermediate unit.

8. (Previously Presented) The method of claim 7, wherein the update information is accompanied by a time stamp for determining whether the update information is still valid when the intermediate unit encounters the second unit.

9. (Previously Presented) The method of claim 7, wherein the delegation of update rights comprises delegation of rights to further delegate update rights.

10. (Currently Amended) The method of claim 1, wherein the assigning step further comprises the steps of:

determining, at an assigning unit in the group, a token secret common for the group and non-correlated with the password; and,

creating, at the assigning unit, the authentication token for another unit in the group based on the token secret and the password.

11. (Previously Presented) The method of claim 10 wherein the step of determining the token secret involves generating the token secret, as a part of an initial set-up procedure.

12. (Cancelled).

13. (Previously Presented) The method of claim 10, wherein the creating step involves using a bijective locking function, the input parameters of which include the token secret and a one-way function of the password.

14. (Previously Presented) The method of claim 13, wherein the locking function is a symmetric encryption function.

15. (Previously Presented) The method of claim 13, wherein the locking function is implemented through password-based secret sharing.

16. (Previously Presented) The method of claim 1, wherein implementing policies in at least one of the units in the group for limiting the number and/or frequency of authentication attempts.

17. (Previously Presented) The method of claim 1, further comprising the step of generating an alarm signal if the number of authentication attempts exceeds a predetermined value.

18. (Previously Presented) The method of claim 1, further comprising the step of sending an authentication response message from the second unit indicating the result of the comparing step.

19. (Previously Presented) The method of claim 1, further comprising the step of authentication of the second unit towards the first unit, whereby the first and second units are mutually authenticated towards each other.

20. (Currently Amended) The method of claim 19, further comprising the steps of:

generating a respective random value at the first and second unit;

determining temporary test secrets at the first and second unit based on the random values; and,

exchanging the temporary test secrets between the first and second unit for mutual authentication purposes.

21. (Previously Presented) The method of claim 1, wherein critical operations for which authentication is needed are listed in policies in at least one of the units.

22. (Previously Presented) The method of claim 3, wherein a unit that is switched-on after being inactive for a predetermined period of time automatically requests appropriate update information from at least two other units.

23. (Previously Presented) The method of claim 1, wherein the group of units constitutes a Personal Area Network (PAN).

24. (Previously Presented) The method of claim 1, wherein the authentication tokens are tamper-resistantly stored in the respective units.

25. (Currently Amended) A communication system including a group of at least two units associated with a common password, and means for password-based authentication, comprising:

means for assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;

means for determining, at a first unit, a check token for a second unit based on the password and the authentication token of the first unit; and

means for comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit;

wherein the means for determining the check token further comprises;

means for retrieving, at the first unit, the token secret using the authentication token of the first unit and the password; and

means for creating, at the first unit, the check token for the second unit based on the token secret and the password.

26. (Currently Amended) The system of claim 25, further comprising;

means for deleting the password and parameters generated in the authentication procedure except the authentication tokens after usage thereof.

27. (Currently Amended) The system of claim 25, further comprising;

means for transferring update information from the first unit to the second unit; and,

means for accepting, at the second unit, update information from the first unit in response to a successful authentication.

28. (Previously Presented) The system of claim 27, wherein the update information is associated with revocation of a non-trusted group member.

29. (Previously Presented) The system of claim 27, wherein the update information relates to a password change.

30. (Previously Presented) The system of claim 27, wherein the update information is selected from the group of : new authentication tokens, a new group key, a group-defining list, and a revocation list, including combinations thereof.

31. (Previously Presented) The system of claim 27, further comprising means for delegation of update rights to a third intermediate unit, and means for sending at least a portion of the update information for the second unit to the intermediate unit.

32. (Currently Amended) The system of claim 25, wherein the means for assigning further comprises:

means for determining, at an assigning unit in the group, a token secret common for the group and non-correlated with the password; and,

means for creating, at the assigning unit, the authentication token for another unit in the group based on the token secret and the password.

33. (Cancelled).

34. (Previously Presented) The system of claim 32, wherein the means for creating involves a bijective locking function, the input parameters of which include the token secret and a one-way function of the password.

35. (Previously Presented) The system of claim 25, wherein policies implemented in at least one of the units in the group for limiting the number and/or frequency of authentication attempts.

36. (Previously Presented) The system of claim 25, further comprising means for generating an alarm signal if the number of authentication attempts exceeds a predetermined value.

37. (Previously Presented) The system of claim 25, further comprising means for sending an authentication response message from the second unit.

38. (Previously Presented) The system of claim 25, further comprising means for mutual authentication between two units in the group.

39. (Previously Presented) The system of claim 25, wherein policies defining critical operations for which authentication is needed.

40. (Previously Presented) The system of claim 25, wherein said communication system being a Personal Area Network (PAN).

41. (Currently Amended) A first device belonging to a group of at least two devices associated with a common password, and including means for password-based authentication, the first device comprises:

means for receiving a password; means for assigning individual authentication tokens to other devices in the group based on the password such that each authentication token is irreversibly determined by the password;

means for determining a check token for a second device in the group based on the password and the authentication token of the first device; and

means for transmitting the check token to the second device for authentication towards the second device;

wherein the means for determining the check token further comprises;

means for retrieving the token secret using the authentication token of the first device and the password; and

means for creating the check token for the second device based on the token secret and the password.

42. (Previously Presented) The device of claim 41, further comprising means for deleting the password and parameters generated in the authentication procedure except the authentication token after usage thereof.

43. (Currently Amended) The device of claim 41, further comprising;
means for creating update information for the second device; and,
means for securely transferring update information to the second device.

44. (Previously Presented) The device of claim 43, further comprising means for delegation of update rights to an intermediate device, and means for sending update information for the second device to the intermediate device.

45. (Currently Amended) The device of claim 41, wherein the means for assigning further comprises;
means for determining a token secret common for the group and non-correlated with the password; and,
means for creating the authentication token for another device in the group based on the token secret and the password.

46-47. (Cancelled).

* * *